SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

INFORMATION SECURITY IN THE ERA OF THE DIGITAL ECONOMY: CHALLENGES AND STRATEGIES. INNOVATIVE APPROACHES TO SOLVING ECONOMIC CHALLENGES

https://doi.org/10.5281/zenodo.11082055

Karabaev Rustam Zafarovich
Tashkent University of Information Technologies,
3rd year student of the Faculty of Economics and Management in the Field of ICT
Saitkamolov Mukhammadkhoja Sabirkhoja ugli
Tashkent University of Information Technologies,
Dean of the Faculty of Economics and Management in the Field of ICT,
Doctor of Economic Sciences

ANNOTATION

The digital economy has brought unprecedented opportunities for businesses to thrive and expand. However, it has also exposed them to new and evolving risks in terms of information security. This article explores the challenges faced by organizations in ensuring information security in the era of the digital economy and highlights the strategies that can be employed to address these challenges effectively.

Key words
digital economy, unprecedented opportunities, information security, evolving risks.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ: ВЫЗОВЫ И СТРАТЕГИИ. ИННОВАЦИОННЫЕ ПОДХОДЫ К РЕШЕНИЮ ЭКОНОМИЧЕСКИХ ВЫЗОВОВ

https://doi.org/

Карабаев Рустам Зафарович
Ташкентский университет информационных технологий,
студент 3 курса факультета экономики и менеджмента в сфере ИКТ
Саиткамолов Мухаммадхожа Сабирходжа угли
Ташкентский университет информационных технологий,
Декан факультета экономики и менеджмента в сфере ИКТ,
доктор экономических наук

АННОТАЦИЯ

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

Цифровая экономика открыла перед предприятиями беспрецедентные возможности для процветания и расширения. Однако она также подвергла их новым и постоянно меняющимся рискам с точки зрения информационной безопасности. В этой статье рассматриваются проблемы, с которыми сталкиваются организации при обеспечении информационной безопасности в эпоху цифровой экономики, и освещаются стратегии, которые могут быть использованы для эффективного решения этих проблем.

Ключевые слова

цифровая экономика, беспрецедентные возможности, информационная безопасность, растущие риски.

RAQAMLI IQTISODIYOT DAVRIDA AXBOROT XAVFSIZLIGI: QIYINCHILIKLAR VA STRATEGIYALAR. IQTISODIY MUAMMOLARNI HAL QILISHDA INNOVATSION YONDASHUVLAR

Karabayev Rustam Zafarovich
Toshkent axborot texnologiyalari universiteti,
AKT sohasida iqtisodiyot va menejment fakulteti yo‘nalishi bo‘yicha 3-kurs talabasi
Saitkamolov Muxammadxo‘ja Sobirxo‘ja o‘g‘li
Toshkent axborot texnologiyalari universiteti,
AKT sohasida iqtisodiyot va menejment fakulteti dekani,
Iqtisodiyot Fanlari Doktori

ANNOTATSIYA

Raqamli iqtisodiyot korxonalar uchun misli ko'rilmagan farovonlik va kengayish imkoniyatlarini ochdi. Shu bilan birga, u ularni axborot xavfsizligi nuqtai nazaridan yangi va doimiy o'zgaruvchan xavflarga duchor qildi. Ushbu maqola raqamli iqtisodiyot davrida axborot xavfsizligini ta'minlashda tashkilotlar duch keladigan muammolarni ko'rib chiqadi va ushbu muammolarni samarali hal qilish uchun ishlatilishi mumkin bo'lgan strategiyalarni ta'kidlaydi.

Kalit so'zlar

raqamli iqtisodiyot, misli ko'rilmagan imkoniyatlar, axborot xavfsizligi, ortib borayotgan xatarlar.

Introduction. The article delves into the various threats and vulnerabilities that arise from increased connectivity and reliance on digital technologies. It discusses the potential economic consequences of cyberattacks, data breaches, and other information security incidents. Additionally, it sheds light on the regulatory

JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

and compliance frameworks that organizations need to navigate in order to safeguard sensitive information and protect their customers.

In response to these challenges, the article presents innovative approaches to solving economic challenges related to information security. It explores emerging technologies such as artificial intelligence, blockchain, and advanced encryption techniques that can bolster the security of digital systems and transactions. Furthermore, it examines the importance of fostering a culture of security awareness and proactive risk management within organizations.

By providing insights into the intersection of information security and the digital economy, this article aims to equip businesses, policymakers, and professionals with a comprehensive understanding of the challenges they face and the strategies they can adopt to ensure a secure and resilient economic environment. Ultimately, it emphasizes the need for continuous adaptation and innovation in order to stay ahead of evolving threats in the dynamic landscape of the digital economy. In the era of the digital economy, where technology is deeply integrated into every aspect of business operation, information security has become a critical concern. The increasing reliance on digital technologies, interconnected systems, and vast amounts of data has brought unprecedented opportunities for economic growth and innovation. However, it has also exposed organizations to new and evolving risks.

Cyberattacks, data breaches, and information security incidents have become more sophisticated, posing significant challenges to businesses across various sectors. The consequences of such incidents can be far-reaching, impacting not only the affected organizations but also their customers, partners, and the overall economy. As a result, ensuring robust information security has become an essential element of sustainable business practices.

Research methodology. This article explores the challenges faced by organizations in safeguarding their information assets in the digital economy and highlights the strategies and innovative approaches that can be employed to address these challenges effectively. It delves into the complex landscape of information security, where technological advancements and the evolving threat landscape require continuous adaptation and proactive measures. By examining the interplay between information security and the digital economy, this article aims to provide valuable insights to businesses, policymakers, and professionals involved in the economic sphere. It emphasizes the need for a comprehensive understanding of the risks and vulnerabilities associated with the digital realm, as well as the proactive steps required to protect sensitive information and maintain economic stability.

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

Through a combination of regulatory compliance, advanced technologies, and a culture of security awareness, organizations can navigate the challenges of information security in the digital economy. By doing so, they can not only mitigate risks but also unlock the full potential of the digital revolution, fostering innovation, trust, and sustainable economic growth.

The digital economy thrives on the free flow of information, but this creates a double-edged sword. While information is the lifeblood of digital transactions, it also becomes a prime target for malicious actors. Here's a breakdown of the key challenges and potential strategies:

Challenges:

- **Evolving Threats:** Cybercriminals are constantly developing new tools and techniques. From sophisticated malware to social engineering scams, staying ahead of the curve is a continuous battle.
- **Increased Attack Surface:** The interconnected nature of the digital economy creates a vast attack surface. Cloud computing, mobile devices, and the Internet of Things (IoT) all introduce new vulnerabilities.
- **Data Breaches:** Sensitive information like financial records, personal data, and intellectual property are highly valuable on the black market. Data breaches can have severe financial and reputational consequences.
- **Insider Threats:** Disgruntled employees, accidental leaks, and human error can all contribute to information security breaches.
- **Lack of Awareness:** Many users lack a basic understanding of cybersecurity best practices, making them susceptible to phishing attacks and other social engineering tactics.

Strategies:

- **Defense in Depth:** A layered approach to security is crucial. This involves firewalls, intrusion detection systems, data encryption, and user access controls.
- **Security Culture:** Promoting a culture of security awareness within organizations is essential. This includes training employees on best practices and fostering a culture of reporting suspicious activity.
- **Zero Trust Security:** This approach assumes no user or device is inherently trustworthy. Every access request must be verified before granting access to systems and data.
- **Data Security Best Practices:** Organizations need robust data security practices, including data classification, encryption, and secure disposal.
- **Collaboration:** Information sharing between businesses, law enforcement agencies, and governments is critical to combatting cybercrime effectively.

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

• **Emerging Technologies:** Technologies like blockchain and artificial intelligence hold promise for improving information security, but their integration requires careful consideration.

Innovative Approaches:

• **Biometric Authentication:** Using fingerprints, facial recognition, or iris scans for authentication can add an extra layer of security.

• **Continuous Monitoring:** Security systems that continuously monitor network activity and user behavior can help detect and respond to threats faster.

• **Security Automation:** Automating routine security tasks can free up human resources to focus on more strategic initiatives.

• **User Education with Gamification:** Using gamified educational tools can make learning about cybersecurity more engaging and effective.

By implementing these strategies and embracing innovative approaches, organizations and individuals can create a more secure digital environment for the evolving digital economy.

Currently, financial institutions are increasingly [1] investing in digital technologies, which provide a number of advantages, including improving the quality of customer service. Data collected through cloud systems, artificial intelligence, and robotics will help financial institutions predict and understand customer behavior and expectations. Financial institutions will have the opportunity to develop and personalize new products and services according to customer needs. Similarly, digital technologies can help in the fight against fraud: according to PwC (2016), financial institutions use AI to detect abnormal behavior, detect market abuse and fraudulent transactions. AI and robotics are also used to protect against cyber-attacks by tracking possible threats and identifying potential security risks. These technologies allow financial institutions to take immediate measures to protect their customers' personal data and account information. In addition, financial institutions have begun to widely implement blockchain technology. Although blockchain technology is often associated with cryptocurrencies, it also has advantages for organizations providing financial services. Blockchain technology allows you to create a distributed database that stores an ever-increasing number of records, and a distributed ledger is constantly updated and synchronized between several computers on the network. These digital technologies also contribute to improving the quality of services, as manual processes are automated and employees can focus on providing more specialized services such as planning, budgeting, taxation and finance. In addition to financial technologies, a number of other technologies belonging to four categories threaten to disrupt and change the growth strategies of emerging economies: according to

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

the OECD classification of amenities, these are digital technologies, biotechnologies, modern materials, energy and the environment. Finding solutions to cybersecurity problems in the digital economy The technologies that can cause the greatest shocks, narrowing some opportunities for developing economies and at the same time opening up alternative development paths, include: robotics and repetitive manual labor the industrial Internet of Things, which will further reduce the complexity of production, monitoring and maintenance, as well as increase the number of factories and warehouses operating without light mobile Internet and increased connectivity, which will allow access to banking, transportation, medical and other services via mobile devices; big data and advanced data analysis; hardware and software as a service (SaaS) and platform (PSP) over the Internet; and the development of a new type of mobile Internet that will allow mobile devices to access a wide range of The range of services, such as These and other technologies that have already become widespread, are mainly improved and expanded by developed countries and adapted to their core assets and capabilities.

Fig.1 Digital resilience [2]

These technologies strengthen the comparative advantages of high-income countries in manufacturing and services, where demand is growing. New technologies can widen the technological and productivity gap between developed and developing economies (Haldane 2017). Indeed, emerging economies face a "perfect storm" if they do not take into account new technological realities, adjust their policies, increase the level of human capital and adapt their institutions. These and other technologies, which have already become widespread, are mainly being improved and expanded by developed countries and adapted to their core assets and potential. These technologies strengthen the comparative advantages of high-income countries in manufacturing and services, which will be in increasing

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

demand in the future. New technologies can widen the technological and productivity gap between developed and developing economies (Haldane 2017). Indeed, emerging economies are threatened by "perfect storms" if they do not take into account new technological realities, adjust their policies, increase the level of human capital and adapt their institutions. Every transaction is recorded, and almost everything can be found immediately on mobile phones. Such massive and widespread use of the Internet raises concerns about the loss of personal data, information leakage and money as a result of cyber-attacks. The nature of cyber attacks has changed: from pranks to deliberate attacks, the most serious of which are pre-planned in order to cause serious damage to someone in the form of loss of money or extortion in the form of loss of personal data.

Fig.2 Digital economy strategies [3]

To protect themselves from ruin, companies must take many serious measures to protect themselves from cyber attacks. Companies are increasingly using disruptive technologies to attract customer attention: according to Hess, Benlian, Matt and Wisbeck (2016), almost 90% of market leaders in the United States and Great Britain want their IT specialists to use the Internet in all models and schemes. They want it. They want their customers to have direct access to them so that they can see their products better. However, they are putting themselves at potential risk as companies are increasingly connecting to each model using wireless technology. Having such access can lead to cyber attacks and loss of corporate sovereignty.

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

The digital economy has ushered in a new era of connectivity, innovation, and economic growth. With the rapid advancement of technology and the widespread adoption of digital systems, organizations are leveraging the power of data and digital infrastructure to drive efficiency, productivity, and competitiveness. However, this digital transformation also brings forth a host of challenges, particularly in the realm of information security. In the interconnected digital landscape, where data flows across networks and organizations rely heavily on digital platforms, information security has become a paramount concern. The potential risks and vulnerabilities associated with cyber threats, data breaches, and malicious attacks have increased exponentially, posing significant challenges to businesses operating in the digital economy. The consequences of these incidents can range from financial losses and reputational damage to legal and regulatory implications. This article delves into the challenges faced by organizations in ensuring information security in the era of the digital economy and explores the strategies and innovative approaches that can be employed to tackle these challenges effectively. It examines the evolving threat landscape, encompassing sophisticated cyber attacks, social engineering tactics, and the risks associated with emerging technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence. Moreover, the article highlights the importance of a holistic and proactive approach to information security. It emphasizes the need for organizations to establish robust security frameworks, implement comprehensive risk management strategies, and foster a culture of security awareness among employees. Additionally, it explores innovative approaches and technologies that can enhance information security, including blockchain, machine learning, and encryption techniques. Generally, a combination of reference cases, primary research, and analysis is used to conduct research on the digital economy, with the data being used to achieve the desired results. In the realm of the digital economy, tourism is a crucial area that can significantly impact economic growth. The use of digital technologies in this field, such as online reservation systems, electronic payment systems, hotel and restaurant management systems, and online tourism services, can enhance the tourist experience and decrease operating costs in the tourism industry. Moreover, incorporating digital technologies like virtual and augmented reality can help attract more tourists, thus promoting economic growth. Several data points related to economic growth and tourism in the digital economy are noteworthy.

SIR Publishers
CENTER FOR INTERNATIONAL SCIENTIFIC PUBLICATIONS
JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

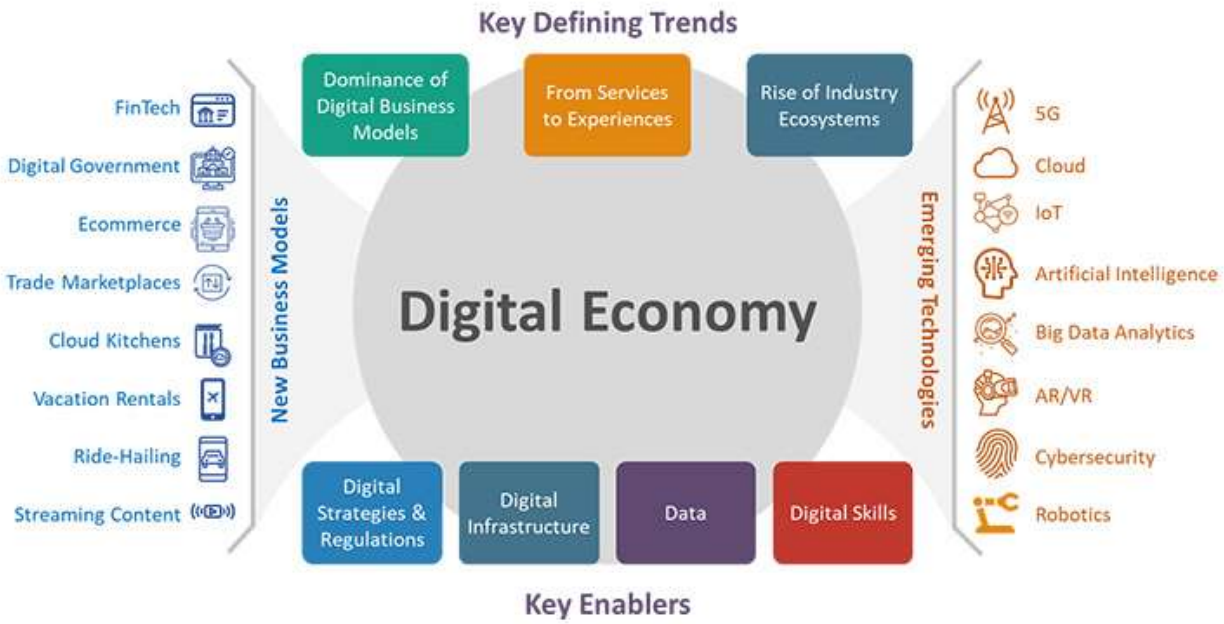

Fig.3 Fields and connections in digital economy [4]

The digital economy requires organizations and individuals to connect seamlessly regardless of their location and therefore relies on robust, reliable, responsive, secure, and scalable digital infrastructure. Digital infrastructure, today, is comprised of a myriad of technological elements such as telecommunication networks, compute and storage infrastructure — including data centers and the cloud — sensor and camera networks, applications and platforms. The evolution of infrastructure is characterized by two overarching trends: the move toward the edge and the uptake of cloud platforms. By the end of 2022, 60% of network resources will migrate to the network edge, to deliver adaptable and agile connectivity services to a population who live, work, and play in a heavily distributed way. At the same time, the shift toward the cloud is helping organizations achieve infrastructure transformation and application modernization goals.

For the digital economy to thrive, continued investment must be made to enhance and upgrade digital connectivity, particularly as technology evolves. Technological advancements such as 5G and Wi-Fi 6 will be key enablers of the new economy in coming years. For example, various organizations are now implementing private 5G networks for different use cases, such as remote triaging in connected ambulances in the healthcare sector, remote surveys by mobile robots in hazardous environments in the energy sector, and factory automation in manufacturing.

According to the World Tourism Organization (WTO) report, in 2019, 1.4 billion international tourists traveled worldwide and generated over 1.56 trillion dollars in revenue. Recent surveys indicate that the use of online reservation

JOURNAL OF ECONOMICS AND BUSINESS MANAGEMENT
ISSN(Online): 2984-7095
SJIF Impact Factor |(2024): 6.563|
Volume-7, Issue-4, Published |20-04-2024|

platforms in the tourism industry has improved the tourist experience and increased the income of tourism businesses. By understanding the challenges and adopting effective strategies, organizations can protect their sensitive data, preserve customer trust, and mitigate the economic risks associated with information security incidents. The article aims to provide valuable insights to businesses, policymakers, and professionals in navigating the complex landscape of information security in the digital economy. It underscores the significance of continuous adaptation, collaboration, and innovation to address the evolving challenges and ensure a secure and resilient digital ecosystem that fuels economic growth and prosperity.

LIST OF SOURCES USED

1. https://www.researchgate.net/
2. https://www.weforum.org/agenda
3. https://digitalregulation.org/
4. https://e.huawei.com/
5. https://www.sciencedirect.com/
6. "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies" by Erik Brynjolfsson and Andrew McAfee
7. "Platform Revolution: How Networked Markets Are Transforming the Economy--and How to Make Them Work for You" by Geoffrey G. Parker, Marshall W. Van Alstyne, and Sangeet Paul Choudary
8. "The Industries of the Future" by Alec Ross
9. "The Fourth Industrial Revolution" by Klaus Schwab
10. "Digital Transformation: Survive and Thrive in an Era of Mass Extinction" by Thomas M. Siebel